PANEL 3 – SECURITY II

Moderator: CAPT Anthony Regalbuto, U.S. Coast Guard

When Bruce Parker and I started planning for this conference program prior to the attacks of September 11, we wanted to have at least one security panel – I guess we thought it was pertinent. Obviously since the attack, the focus of the entire nation has been on security issues, making this conference panel discussion very timely. I will provide you with an overview of how the Coast Guard has been approaching these security issues and initiatives. This will help set the context for identifying the technology and research security needs from the Coast Guard's perspective. Other panelists will hopefully outline their own technology and research needs based upon their own experiences.

Within the Coast Guard, the concept of security is being addressed through a "family" of security plans. We envision a port security plan as the umbrella plan for the entire port. In addition, we will require vessels, facilities, and offshore platforms to have specific security plans. The model we are using is very much like the area, vessel and facility plans developed for oil spill response following the EXXON VALDEZ oil spill. We have had great success with this approach and it makes a lot of sense from the standpoint that the plans are integrated and layered depending upon the threat.

We have developed an external threat advisory system for the maritime industry. Most of you have probably heard of threat conditions and forced protection conditions, which are internal conditions for military installations to provide different levels of physical protection based upon threat. We needed a layered protective system for the public sector so that the appropriate level of security activities could be undertaken for the given threat. These new threat conditions are Maritime Security Levels 1, 2 and 3: level 1 is what we term "new normalcy"; 2 is heightened risk; and 3 is incident-eminent or under attack. As the Captain of the Port (COTP) receives threat information relating to a particular port, he or she can then set a threat condition for the port and inform everybody in the port to execute their plans to the corresponding Maritime Security Level.

I want to reiterate that Level 1 is "new normalcy" and we will not be going back to what was considered normalcy prior to 9/11. Our world has changed and we must change accordingly. Unfortunately, our port security will be at a much higher level than before since terrorists have demonstrated that they can use our transportation system to deliver weapons of mass destruction.

One of the issues that we've been wrestling with is the issue of critical infrastructure protection (CIP). As part of the tasking following the 9/11 incidents, one of the things we had to do was try to identify the "critical infrastructure" in the maritime environment. Coast Guard Headquarters directed all of our COTPs to identify the critical infrastructure in their respective ports. For the Coast Guard, we identified over 1,000 pieces of critical infrastructure just in Tier 1, which is the high-risk and high-vulnerability, which clearly makes CIP an issue for the Coast Guard since we do not have the resources to protect all of this infrastructure.

In addition, as part of an USDOT-wide effort, I was assigned to work with the Secretary of Transportation's key staffers and the other modes to identify critical transportation infrastructure system-wide -- we identified more than 50,000 elements of critical infrastructure within the nation's transportation system. When our CIP was added to other agencies like the EPA and the Nuclear Regulatory Commission, it was clear as a nation that we have thousands and thousands of critical infrastructure elements. It became obvious that we, as a nation, are very vulnerable and we are obviously going to have to come up with a scheme to protect that infrastructure.

Currently, the Coast Guard has a force of 35,000 people, the level at which the agency was in the 1960's. This reduction has resulted from streamlining and leaves us with a force that is smaller than the New York City Police Department. Certainly, we do not have the resources to protect all critical infrastructure that has been identified. Therefore, the owners and operators of the infrastructure will have the primary role to provide for their own protection. Through USCG roving patrols, we will ensure there is an adequate level of security at the facilities. If security is found to be inadequate, we will engage with the owner or operator to improve their security posture. We have broad authority and if necessary we can control operations or close the facility so the owner and operator can implement appropriate security measures.

In some port areas, there are a few pieces of critical infrastructure that if damaged or destroyed could close the port for days or weeks. I can think of several examples. In New York, it could be the Verrazano Narrows Bridge -- Admiral Bennis, Captain of the Port in New York was so concerned about the security of this bridge that he provided Coast Guard resources to protect it on land and on the water. In California, the Golden Gate Bridge would be another example. I am sure most of you can think of other structures in your ports if damaged, all port operations would probably cease.

Another important area that we are working on is the methodology to conduct port vulnerability assessments. This is something that was underway prior to the incident, although folks in Congress and the industry were not all that interested. Even within the USCG, these assessments were relatively low on the list of priorities when we were trying to get funding for it. Following the incident, Congress and industry representative now want to know how many assessments we can do and how quickly we can do them. They essentially are asking "Can't you do all 362 ports in one year?" My response is simply I don't think so. This is going to be a major challenge for us. Our approach has been to identify those ports, which are militarily or economically strategic ports of the United States. We have identified about 55 ports, which handle about 95% of the international trade by sea. We have presented the list to the Commandant and, once approved, the list will be shared with the industry and Congressional staffers. Because it is going to be a contentious issue with the ports, my approach is going to be to put it in alphabetical order so the port representatives will know if they are above or below the cut. Obviously, every port is going to wonder why they are not number one or whatever standing; however, from my standpoint, this should not be an issue. The important point to remember is if you are on the list, you're going to get an assessment.

We also developed an initial assessment tool that will soon be available to our COTPs. For those assessments that don't require the special expertise that the more comprehensive inspections will require, we have developed this new tool to identify vulnerabilities. The tool is driven by different potential terrorist scenarios, which are weighted and scored to identify the highest risks in the port. The COTP can then target his/her limited resources against the highest risk. Additionally, as mitigation efforts are identified, they can be plugged back into the methodology to determine how the measures are going to score out and whether or not the measures are really having the desired risk reduction. It will be a very useful tool for the Coast Guard and port stakeholders.

We determined the tool does not need to be classified; however, once you populate it, that information is very sensitive and will be classified. It would behoove people in the ports that need to be "in the know", to get their security clearances so they are allowed to review classified material.

One of the things we need to address for the future is our ability to surge activities for higher levels of security; we don't have the resources to sustain operations in a port. We are marginally able to do so now by using our deployable port security units that were established to provide force protection for military installations overseas. We have called up our Port Security Units made up of Reservists in four of our major ports to provide this surge capability. We are presently designing new maritime safety and security teams mostly made of active duty people. They will be available to deploy in a short period of time for special operations in any U.S. port, They will also help in the port vulnerability assessments and the follow on port security exercises. This is important new resource for our Coast Guard.

Immediately following the attacks, we initially thought the threat was from outside the country. Therefore, most of our initial efforts were focused on our coastal ports. As we began identifying our vulnerabilities, we recognized that our inland river system and Great Lakes region was also at risk from potential terrorist cells already in the United States. It is much easier to get on a towboat with its low freeboard compared to deep draft vessels. Also, many of the barges on the river system carry hazardous chemicals that could be exploited by terrorist cells. We will have to provide some type of law enforcement resources on the river system in addition to the coastal ports. We have already developed the concept of a Sea/River Marshal modeled after the airline industry. They will ensure positive control of the vessel so that it can be navigated safely in U.S. ports. Hopefully, we will get additional resources so that Sea Marshals can be provided on those vessels carrying cargos, which can be used as weapons of mass destruction..

One of the things that the Commandant and Steve Flynn mentioned yesterday is the concept of maritime domain awareness; a concept that we have been pushing in the Coast Guard. We want to push our maritime borders out, away from the coastal United States and really have a better awareness of the people, cargo and vessels that are coming to the United States. Part of our strategy as the incident was unfolding, was to use our existing regulations, which requires a 24-hour advance notice of arrival for vessels. We issued a temporary order, which required the crew and passenger list in advance as part of that advance notice of arrival. We then issued a temporary emergency rule, which required the arrival information 96 hours in advance. This gave our analysts more time to screen people and identify potential terrorists. This has been very helpful in our efforts to improve maritime domain awareness.

Another problem that came to light is we don't have one Federal database to screen for terrorists. Apparently, there are several law enforcement and intelligence databases. These systems need to be fused so when we run it we have a level of confidence that we've hit all the databases to ensure no one slips through the cracks.

One of the other major issues that we need to tackle is the credentialing of people. The USCG believes there is a need for some type of smart card with biometrics in the card that ties the individual to the card. As someone tries to gain access into a facility or onto a ship, the process would provide a reader with the ability to read the smart card and determine if the identity of the person is the same as the card. The problem with this approach is that our transportation system is made up of many modes. If we do implement something like this, it should be for the entire transportation system so that workers from one mode may gain access to another mode as the cargo is moved throughout the system. Just as longshoremen work at port facilities, trucks drive onto the same facilities and we certainly want to have a level of confidence that the person driving the truck onto the facility has been screened for entry as the longshoremen arriving for work.

The other part of the equation that leaves a security gap are the seaman coming from overseas. From a safety concern, we currently don't have a level of confidence on their credentialing as far as licensing, and skills and ability to operate the ships. We trade with many developing countries and currently there are many cases of fraudulent documents. We need to close that loop to ensure that people coming to the United States have been screened, and properly identified. Think too about all the millions of cruise passengers coming into the United States each year with possibly fraudulent documentation. If they haven't been properly screening too, they may present a major security risk to our country.

Another thing we need help on is the CBRN detection equipment – chemical, biological, radiological and nuclear. We need to have the capability to better screen cargo as it is coming into the United States. It is really too late when a container shows up on the pier in the United States. It may be too late at that point, particularly if there is a GPS firing device on the container box. As it reaches a predetermined coordinate, the bomb could explode or the chemical dispersed. We need better domain awareness of the cargo entering our country and we need to work better with U.S. Customs and work in partnership with other Customs Services on proper chain of custody of containers from the point of origin to its final destination.

By working through the World Customs Organization and through IMO, I think Coast Guard, Customs and INS can help ensure a consistent level of security in other countries commensurate with ours. Our approach really has to be at the point of origin – where the box is being stuffed – to ensure there is adequate security on that container and that the container is being sealed and that we have a chain of custody as the container moves through the transportation system. We need to know with some level of confidence that the container holds the cargo that is represented on the paperwork. We need to have back-up detection equipment available so as the crane is picking up a particular box, the detection equipment is on the crane and is actually screening it for CBRN so that we have some level of confidence that the container is in legitimate trade or not. Looking to the future, we are even thinking about having the ability to read the ship at the sea buoy, to see if there are weapons of mass destruction on board that ship. That is the level of detail we are trying to address with these issues. Now, let's move on to our panel.

Our first speaker will be John McGowan. John is the Executive Director of Enforcement and Planning of the Office of Field Operations in the United States Customs Service. As the Executive Directory, he is responsible for providing national direction, development and implementation of the Customs Service core business of outbound cargo and travelers. Mr. McGowan administers to the Office of Field Operations aspect of National Narcotics Enforcement, Planning and Strategy. He has served as the Executive Directory of the Interagency Commission on Crime and Security in U.S. seaports, and that report is more valid today than when we actually did that study, and opened a lot of eyes to the issues. Mr. McGowan received his BA from Hunter College, New York City, and was a Senior Executive Fellow at the J.F. Kennedy School of Government, Howard University.

Our second speaker will be Mr. Keith Seaman. Mr. Seaman is Chief of Concept and Technology Team, Plans and Policy Director of the United States Transportation Command, Scott Air Force Base in Illinois. He was recently promoted to GS-15 and selected for Senior Executive Service school at the Industrial College of the Armed Forces. He is responsible for the USTRANSCOM's Joint Transportation Technology Office.

Our third speaker, Mr. Carl Trovato, will offer an industry perspective. Mr. Trovato has over 35 years of experience in the marine transportation industry. He has been with the Philadelphia Regional Port Authority as a Director of Operations in the last 13 years. In addition to his present position, Mr. Trovato served as Cruise Terminal Operations Consultant to the Ports of Philadelphia and Camden. Prior to his present place of employment, he was with the United States Lines for 22 years in various supervisory positions. He has also served three years on active duty with the U.S. Coast Guard.

Our fourth speaker, Mr. John LaCapra, will tell us about Florida ports, which may be a model for some of the things they have done. Mr. LaCapra is a private attorney with nearly three decades of international business, seaport development, and cruise industry experience. He is President of the Florida Ports Council, a statewide management organization comprising 14 deep-water ports. Mr. LaCapra is also special counsel to the International Council of Cruise Lines.

Our fifth speaker will be Mr. John J. Lynch. Mr. Lynch is a structural engineering working in the Naval Facilities Engineering Command, Engineering Innovation and Critical Office located at the Atlantic Division in Norfolk, Virginia. He is responsible for the technical adequacy of all Naval shore facility engineering, design and construction criteria, which includes unified facility criteria and unified facility guide specifications.

The final speaker will be Mr. Raymond Barberesi, Director of the Maritime Administration's Office of Ports and Intermodal Development. Ray is a member of the federal government's Senior Executive Service at the U.S. Department of Transportation.

John McGowan, Executive Director,

Enforcement Planning, U.S. Customs Service

The report from the Interagency Commission is as valid today as it was when it was issued in September 2000, with the single, notable exception. In that report, what we said was the terrorist threat in U.S. seaports is low and the vulnerability is high. I think the threat has changed. The vulnerability probably has not. That is what is getting a lot of attention in a lot of circles in the United States today, both in the Congress and in the Administration, within the private sector, within the transport industry at large – each of the pieces of the chain.

Tony talked about what the Coast Guard has done behind 09/11. U.S. Customs is responsible for 301 ports of entry in the United States. The ports are seaports, airports, land-border ports, and inland ports. We have ports where no foreign arrival occurs. We have what is called inbound ports – goods move there under Customs custody and under Customs control, but in the care of a carrier who may or may not have been a foreign arrival. All of these are points where we had to start refocusing some of our initiatives and our efforts.

At the same time we were doing that, we got a levy from the U.S. Marshall Service, which had gotten a levy from the Department of Transportation/FAA to provide law enforcement response to airport screening points. We dispatched on the order of 800 inspectors to that levy. We have since been relieved of that by the National Guard. We dispatched 125 inspectors to the northern border to some of our smaller ports. We have ports on the northern border that have one Immigration inspector or one Customs inspector for two shifts and then shut down. The way they shut down is they put up the yellow cone in the lane with an arrow – please report to next open port of entry to the left. The border patrol on the northern border had something in the order of 500 persons assigned to control through patrol between ports of entries. There are 143 crossings on the northern border that are marked “in control by U.S. Customs and Immigration”. There are another 600 known frequent crossing sites. That was a major initiative for the agency and for the U.S. government in the short term. At the same time we were trying to control the out-ports, we were also trying to figure out what to do in the major transit points like Blaine and Detroit and Buffalo. I think you probably read headlines that said we had extended 20-minute delays to 8-hour and 15-hour delays because we were searching cargo, when in fact we weren’t searching the cargo but the conveyance. The northern border has represented a low-risk for Customs as far as trade compliance. We have very high trade compliance between Canada and the United States. We have a low risk for narcotics. There is a developing risk for marijuana, or B.C. Bud grown in Canada. But, that is localized to the far western ports.

On September 11th, the major concern became who are the entrants? What is the identity of the people who are coming into the commercial lanes? A lot of those trucks have a driver and a helper. On the southern border, because of the immigration issues on the southern border, trucks usually come in with just a driver and the helper has to come off and walk through the pedestrian lanes and go through immigration screening directly. It wasn’t that way on the northern border. Things changed on the northern border. I don’t think anybody was ready for the changes.

We have returned to some level of normalcy, I think. We have the waits down to what is acceptable to the just-in-time inventory procedures. I think the big three automakers typically have a 3-8 hour inventory on the shop floor because they are getting continuous deliveries from

Canada. When the wait times went from 20 minutes on a dispatch, the second section of parts, to a 16-hour wait, they were losing their capability to keep productivity up. That was a major concern and we reacted appropriately. I think we acted appropriately on 09/11 even two hours after the event, and I think we reacted appropriately on 09/12 when we started making plans to be able to accept that kind of cargo as quickly as we had been before.

Today, we are here to talk about seaports. I want to stress the point that within Customs, we have very broad and large responsibilities. After 9/11, we accomplished a lot by refocusing our narcotic interdiction capabilities as well as our trade fraud screening capabilities and started looking for different risks and different cargo. This is what I will focus on today.

On a typical day in the Customs Service, the workload is substantial. For example, on the air side, on an annual basis, we handle 80 million arriving passengers. This translates to 839,000 commercial aircraft; and another 125,000 private aircraft. On the land environment, we process over 400 million persons arriving by the land borders. We process over 130 million vehicles, over 2.5 million rail cars, and over 11 million what we classify as trucks. On the land border, those trucks could be trucks or sea containers on chassis. In the vessel environment, 11.2 million persons, about half of those are passengers on passenger liners and cruises in and out, U.S. origin back to the United States after a foreign visit. We have about 5.7 million containers on an annual basis. That is a different number than you hear from other people. The American Association of Ports Authorities talks about container movements in terms of 20-foot equivalent units (TEUs). Customs counts actual individual containers. For example, for AAPA, if you took a 40-foot container off of a vessel and went across the dock and put it on another ship of the same line, that would be four movements – two TEUs off and two TEUs on. For Customs, it would be one movement. This accounts for some the disparity one sees between Customs data and indusry data. When we count actual individual containers, we are trying to count the workload, hence the number will differ from AAPA statistics.

Of the total 301 U.S. Customs ports of entry, over 90 of those are seaports. Customs "ports" are counted a little differently they are by USCG or AAPA. When the USCG counts ports and AAPA counts ports, they count those entities that are in control of the port. U.S. Customs counts collection districts. For example, while USCG and AAPA count the Port of Beaumont (TX) as a separate port, Customs includes the Port of Beaumont, the Port of Orange and the Port of Trinity as a single port because all are part of a single collection district. In some cases, the reverse is true. For example, the Port Authority of New York and New Jersey may count as a single port, but the local entities talk about the Port of Newark and the Port of Elizabeth and the Port of New York. At Customs, we talk about the New York port versus the JFK port. For us, the New York port is the Newark Airport plus all of the seaport facilities. While we share information and resources among these kinds of things, it makes for a challenge when trying to track what is going on in the real world.

With 5.8 million sea containers, 98% of all the sea containers arrive at the top 30 ports; 83% of them arrive at 10 ports for Customs purposes. This means Customs puts a lot of resources into those 10 ports. We put a lot of our technology in and our information demands on those 10 ports.

Who do we deal with? There are 491,000 consignees – that is the importers of record. Those are the people who cause the goods to come from foreign places – they order them or accept them from delivery. One third (33%) of those shipments by value is entered by 100 consignees. U.S. Customs has pushed mightily on those top 1,000 consignees for compliance. We're trying to get them into a condition where we can put them on automatic, put them into a low-risk category so we can start dealing with the others. Of the 491,000 consignees, 197,000 are one-time importers. We only see them one time. A lot of that is in the air courier and overnight express business; however, they represent probably the least known. The good news is they are buying from manufacturers whom we have identified and compiled track records on because they are selling to the same people who continuously bring in the goods. Through our tracking systems, Customs can establish relationships between importers and exporters, between manufacturers and consumers. In this way, we can assess risk – how often have we dealt with this person over the last five years and what has their performance been?

Prior to September 11th, we were focused primarily on contraband coming from narcotics source countries – high risk countries for source or transit of narcotics. Post September 11th, we started changing our focus to look for not bank haven countries for narcotics money outbound, but bank haven countries for terrorist activities -- monies coming out of the United States and being used to fund terrorist attacks either here in the United States or other places abroad. We started looking more intensively at what was coming from countries that were known to be at-risk for Al Qaeda support and cells.

The DEA map was our threat prior to 09/11, and was focused on the 16 source in-transit countries for the most part in Central and South America. About 40% of our cocaine threat and heroin threat from those locations comes across the Caribbean by water and by air, and 60% comes through the land borders of Mexico. For the most part, it was originating out of South America. A single source for cocaine is only grown in the Andean regions. Heroin is big in the United States – we consume about 10% of the worldwide heroin production. Most of the consumption is met with demand coming out of Colombia. Colombia has replaced Southeast Asia and Southwest Asia as a source for heroin in the United States. We still see some of that Southwest and Southeast Asian heroin, but we don't see it often. It has been replaced by Colombian heroin for the most part.

Our threat after 9/11 is based on a map from the Department of State. It was put together to indicate where terrorism occurs. Colombia has the highest number of terrorist events – 152 were against the Keo-Ramone pipeline by the National Liberation Army (the ELN), which accounts 86% of their events. What you can see from the map is a relatively placid world before 09/11 as far as terrorist events, or at least what are reported as terrorist events. The definition for terrorism for this kind of a report is "politically-motivated, violence perpetrated against non-combatant targets by sub-national groups or clandestine agents usually intended to influence an audience". International terrorism involves citizens or the territory of more than one country and a terrorist group is any group practicing or that has significant sub-groups that practice international terrorism. There are a lot of gray spots on the terrorism map, which means those areas have not had an event or they did not report an event. I suspect there is more gray area because of reporting failure than because of non-events. There is an awful lot of domestic terrorism occurring in a lot of countries.

I want to also talk briefly about automated targeting systems. Customs has an automated targeting system that mails the information we get from carriers on manifests and from the importers on entry documentation they present when they bring the goods into the United States. We sort through that and make decisions on what we're interested in and then start applying screening capabilities against that which is human intervention. We use analysts and technology, then we do physical examinations. Because a physical examination of a 40-foot container will take 3-5 hours and will involve 3-4 inspectors, we don't have the capability to do a large number of those.

Before 09/11, we built an awful lot of technology that was looking for trace amounts of narcotics on the outside of containers, trace amounts of narcotics on the outside of packaging. We also developed a lot of imaging systems, looking for anomalies in the container structure or if you are looking at homogeneous cargo and everything is square and there are a bunch of round things on top, if you want to know why the round things are there, then you open it up and look into the container itself.

What we need now is more technology to identify chemical, biological precursors or the contents of weapons of mass destruction themselves. We have a lot of technology out there that can be re-set. We do have personal radiation detectors that look like a pager on a belt, which go off when in the presence of a radiation source. We have isotope identifiers, which are brought into an area to determine what you are reacting to. We have a lot of detectors reacting to cancer patients who have just gone through radiation therapy; however, that has a different isotope than what we're interested in and weapon-grade uranium or weapon-grade systems. The isotope identifier and the x-ray tells us what is inside the container without us looking at it – not so much what is inside, but how it is packaged and what it looks like inside.

We are developing some portable gamma imaging systems, which will be a hand-held x-ray that we can use as we go through container yards and look at certain parts of the container. This will be excellent for ro-ro cargoes when you're looking into air tanks and things like those that hang underneath the ro-ro conveyances themselves. We are developing a portable system for this purpose.

Container selectivity is another aspect of inspections and can be represented as a funneling process. We get 5.8 million containers and the first thing we do is we screen it. I talked about AMS – 98% of the manifest information comes to us electronically prior to the arrival of the vessel of between 48 and 24 hours in advance. Those systems match the automated broker information system – that is the automated cargo system, the automated commercial system. When we marry them up in the automated targeting system, we look side-by-side – what is on the manifest and what is the carrier telling us he is carrying, and what is the importer telling us he is entering into the commerce via the United States. We marry that up and we look against our indices to see if we have any past track record with these people about how their performance has been. We make decisions on whether or not we are going to have an intervention for narcotics. We can do the same thing once we start populating these systems with criteria and parameters that address threat for terrorist events.

In the container screening area, we have the non-intrusive inspection technology and large-scale x-rays that we drive the containers through, or large-scale x-rays that are moved over the container. VACIS (vehicle and cargo inspection systems) are based on gamma ray technology. They can be put into permanent systems or they can be put into relocatable systems or they can be trucked down and are fully mobile. We are starting to see a lot of those. That is our preference because we can move them into any terminal or port. In a port like Los Angeles or Newark, where you have multiple terminals, putting a fixed inspection facility into each one of those terminals would eat up a lot of land and I don't think it would be welcome. Nonetheless, ports have to make room for us in some of these places because they are that big and they have that kind of threat, and we are going to need inspection space.

The final thing I want to talk about is physical inspection facilities – centralized examination stations where we relocate the cargo and actually do a thorough physical examination. It ranges from 2-3 hours, depending upon the kind of examination we do and the actual cargo. We are also looking for tools that will allow us to scan the contents of containers after we started entering them. John Pinella is our Executive Director of the Office of Applied Technology and he is our "whiz-bang guru". Anything we get, we take over to him and he has the discipline and the science to evaluate it. He puts it through a the testing regimen before we order and implement. Our inspectors like technological stuff they see in newspapers and they see on late-night T.V. and they want to buy a whole bunch of them. However, we really have to put it through a regimen to make certain it is inspector-proof. It used to be fool-proof, but we have to make them inspector-proof as well. Inspectors are harder than fools in some instances. I used to be an inspector, so I can talk this way – but nobody else can.

If I had to sum it up – we need more information so we can do more screening in advance. We need more technology that we can do more – like that 5.7 million containers, maybe like a half million should go through some sort of screening system because we are going to have concerns about a half-million of them. But, we don't need to put a half-million of them through a CTS. We have capacity for about 100,000. That is what we did last year. I think maybe that is what we should do next year and every year in the future. But, we ought to start changing the focus. We ought to start making sure we have more information, more capability when we do the screening.

Captain Regalbuto talked about defense in-depth. Moving the inspection point, moving the security point further out. We've been trying to do that through information technology. Let me share a quick story. In 1974, inspectors were looking at air cargo in San Francisco Airport and with one inspector a light bulb went off. IATA has standardized air waybills. The air waybill is cut by the air carrier before he receives the freight and it is available in the cargo shed or the cargo room at both airports – the sending airport and the arriving airport. The paperwork was there usually in advance of the aircraft. We started screening the air waybills rather than screening the entries because we had the air waybills before we had the entry. We started doing that in a vessel environment and we were very successful. We started looking at who the people were shipping from and to, what their relationships were through time, what our relationships were with them through time. We automated that process through the 80's. In the 90's, we started adding technology into this.

Ten years ago on the Southwest border, we found very little narcotics in commercial cargo because commercial cargo was just blowing through the import yard. That is where we had more control than anyplace else, but we had more difficulty trying to get them devanned and looked at than anyplace else as well. We added a significant number of dogs and a significant number of new pieces of equipment down there. We have 65 pieces of equipment, most of which are on the Southwest border. We now make 125-130 major seizures out of commercial conveyances on the Southwest border.

Friday of last week, on the 9th of November, we encountered 5,500 metric ton of marijuana, all concealed in modified containers and modified trucks. It was in the ceiling, in the floor, in false walls and in the front of the container. Most of that was discovered through the use of VACIS because the image pops up nice and clean. I suspect that we're not going to have as many people involved in trying to get weapons of mass destruction into this country as we have trying to get narcotics into this country. But, it is the same kind of concealment methods. It is the same smuggling techniques. It is the same people. The people who are shipping goods out of the Middle East, which now contain heroin for consumption in Eastern Europe and Western Europe, are the ones we are going to be sending other payloads using the same methods they use for their illicit narcotics. That is what I think Customs brings to the table.

Our experience with getting more information has been good. Our experience with putting more reliance on foreign security hasn't necessarily been as good although we have had some success in that. We have a lot of success in collecting information from the commercial partners. However, when we rely on them to screen themselves and rely on other people's screening foreign cargo, what happens is they become targets. If we do less examinations on those shipments, they become targets for people who want to take advantage of what they perceive is a free pass into the United States as a means to get their goods into the United States as well.

When I talk about the commercial carriers and the commercial entities who are involved in these seizures on the Southwest border, it is in the Fortune 500 that we are finding marijuana and cocaine; however, it is not the Fortune 500 smuggling it. People are using their conveyances and using their shipments and contaminating them with their contraband.

Thank you.

Keith Seaman, Chief of Concepts and Technology,
U.S. Transportation Command (USTRANSCOM)

I appreciate the opportunity to speak this morning. In today's business world, as far as transportation is concerned, we must look at where we need to drive the research and development for the future. Today, I am going to be speaking mainly from a DOD perspective regarding transportation and logistics. There is a very minor amount of R&D that is being done in the transportation business. The focus of USTRANSCOM is how to drive that as it projects force through the commercial industry today and gets things to the fight.

If you look at how we are doing business today in Afghanistan, we are doing a fairly decent job. However, we must do our job better in the future, especially in light of the fact that we are going to have to project force more rapidly than we did last time. In Desert Storm, it took us six months to get set up and ready to rock-n-roll and this time it took us about 30 days to set up and rock-n-roll and we want to be talking about five days to set up and rock-n-roll in the future. How are we going to manage that kind of force projection and be efficient and effective when we do that?

We have to look at the operational environment for the future that is based on our national security strategy. That national security strategy as seen today is that we have to have forces in place in 96 hours or we have to have bombs on target in 48-72 hours and then be able to sustain those things, or put 40,000 screaming Marines in place in seven days. I don't know about the rest of you, but I don't think our transportation system, whether it is military or commercial, can handle that kind of capability. Given that reality, where is the technology investment that needs to be made in the future? If you look at how we are going to do our business using a national security strategy, being driven by the national military strategy, then looking to the Joint Vision 2020 which sets those things, we have to be able to project force from the earliest stages. We are losing all of our overseas locations and with that in mind, how are we going to get out of our bases faster in the future and be able to push it through our own commercial industry, which is a little bit more robust than most nations on the other side, and then be able to project force out of this robust transportation capability in the United States into a very minor capability in some of those overseas locations? That's what we have to be able to do.

To do that, we must look at the technology investment from an end-to-end perspective. Though the concept is sexy, you cannot just look at high-speed sealift ships. You must look at high-speed platforms, whether they be sea or air. You have to look at the overall transportation situation and all the installations, and then determine how you "get out of Dodge" fast. Our getting out of Dodge fast is the same as the commercial industry's ability to get out of the depot fast so that product gets to the customer real fast. All you have to do is flip around with the commercial and the customer and do it for the DOD. We have a customer out there. He is a soldier or she is an airman, and they have to get there quickly so that they can wage war. You have to look at those four key areas because on top of that is the information technology or the business support that need to be developed to manage that kind of a robust, rapid capability. Woven through all four key areas is the security that is needed to be able to do that.

Technology is exploding. It is multidisciplinary and it must be done in concert with each other. If you are going to build high-speed sealift ships, you have to build agile ports. If you are going to build agile ports, you have to build rapid deployment capabilities or rapid road systems or rapid rail systems. If you are going to do that, then you have to build the IT systems or the to be able to do that -- it has to be multidisciplinary. We can no longer be surprised about technology in the transportation arena. We have to invest in R&D. Right now, we are looking at how we can establish our own R&D budget at USTRANSCOM, because currently the services update did not do a very good job as far as investing for R&D for transportation.

One of the things I have learned about the transportation and logistics community is that they are often dull and sometimes complacent. As a result, they sometimes listen only for what they need to hear about. I have found that you need to have some kind of euphoria and you cannot be caught in complacency as far as technology is concerned. We have to not just get over the speed bumps for those complacent people, but we have to break through the barriers because if it isn't broken, it is about to be broken. Technology is overcoming us and we cannot be technical cynics.

Over the past decade, USTRANSCOM and our commercial partners have done a good job as far as developing those sexy things, such as the LMSRs or large medium speed ro-ro ships or roll-on/roll-offs, the fast sealift ships, C-17's, etc. We are doing a good job in managing those things. The question now is where do we need to go in the next decade? The next decade will demand that we do things better intermodally. This is an end-to-end system.

As I mentioned earlier, we have to put a brigade size force in place in 96 hours; a division in 120 hours; five divisions in 30 days. How many of you believe that our current transportation capability can do that today? You're right – it can. Then, on top of that the Marines say we want 40,000 screaming Marines in place in 7 days. On top of that the Air Force says that we must have bombs on target in 48-72 hours to sustain a movement of five AEFs or air expeditionary forces in 15 days and then there's Navy requirement. That's what the requirement is going to be in the future. We've got to have the right kind of support tools and the capability to project that kind of force for the future.

If you're going to do that, you've got to look at it from an end-to-end, from six months in Desert Storm to 30 days now, to where in the future – five days. How can we do that? It is going to be based on looking for opportunities within the entire process of moving people and things. The process as far as the DOD is concerned is much the same as in the commercial industry. How do we find different ways in which to bypass levels of command and start to do things quicker and eliminate the bureaucracies, eliminate paperwork, and achieve customer satisfaction earlier in an effective and efficient defense transportation system for the future?

To be able to do that, you have to maximize throughput and minimize the handling. Let me just give you an example. The C-17 . . . . . . in the United States where there is no standard on which to develop those things. Why can't we get the major technology companies in the United States to develop and adapt to a specific standard? I have a cell phone right here and it is made by Motorola. Some of you probably have a different type, but they are all built to a certain standard. Why can't we do that so we can communicate and pass data as is necessary for an efficient and effective DTS for the future? You have to look at how do we do loading and offloading of rail. How do you do an efficient marine terminal, like in Tacoma and Seattle? You have to look at the whole end-to-end process, even in the seaport. If you move from the seaport, what we are looking at is how do you take those technologies and develop a port-in-a-box capability.

When we leave out of our . . . . site, . . . already mentioned, it is very robust. If it is very robust, on the other site it is very minimal. For instance, East . . . ., anybody have anything to do with East Seymour – a little tiny pier, ... and we had to put forces inside of there. We have to be able to have the ability to have a port break-out package so that when we get there, we can move things rapidly to the front.

Let’s look at air because it is not only the seaport. We have to link air and sea together. Today our customers sometimes demand that we send everything by air. We have to change that kind of mentality. At USTRANSCOM, we are developing the capability in which WE will make mode determination, not the customers. How many of you go to FedEx and tell FedEx that you want your box of cookies sent to Grandma’s house tomorrow by 10:00 a.m. and use a ship? Do you know what FedEx will tell you? I’m sorry – I don’t care how much money you’re going to give me – I’m not going to do that. Well, today, we have our customer telling us how to do our business at USTRANSCOM. You have to link air, sea and ground together. It cannot be a stovepipe approach. You have to look at all the different ways by which an aircraft can be loaded and offloaded faster because today, a C-17 is 2.5 hours; a C-5 is anywhere from 3-6 hours, depending on who is doing it. We have to be able to do those things. How do we weigh, measure, pack and provide shipper information? We did this back in 1998 and . . . . do this kind of technology in place because we are not using the investment dollars in order to make that happen. We are talking about information and how to get accurate data and yet . . . . when the rubber hits the road, do we really want to invest in the technologies to capture accurate data in the transportation community?

Today, we have developed that kind of capability to reduce from 1,500 vehicles in 125-250 hours down to 25 hours and we reduced the manpower from 5 to 2. Those are the kinds of technologies we need to invest in in the future.

We need to look at the new virtual intermediate staging based technologies. With the United States, as we have lost those opportunities in overseas locations, and when a country says to us, okay, you can come in and you can use only this portion – how do we set up that little tiny portion that they have given to us? We are looking at intermediate staging based technologies for the future.

Now let me shift to the command and control capabilities. USTRANSCOM is establishing a futuristic command and control ACTD or advanced concepts in technology demonstration. It is a four-year, $45 million program that Congress will vote on in two weeks and I’ve been working on this for three years and I’m excited about it. For the first time, USTRANSCOM will have the set of support tools in order to manage the DTS from the very beginning to the end in mode determination and optimization and scheduling for the effectiveness of the DTS. We will work on a collaborative web-based system that is interactive and has fused data so we can have an information visualization picture that we can push to our customer. These technologies are right there today.

As we go forward and especially in light of what has happened overseas, now we also have to look at security. The types of security technologies that we need to invest in include those that allow us to monitor things that are coming into the United States, as well as those being exported from the United States. Some may ask, why the concern about exports? The VISA program (Voluntary Intermodal Sealift Agreement) is where the military cooperates with our commercial partners, who earmark certain portions of their shipping capacity for the DOD. If somebody knows what we are going to do with, for example, a 6,000 TEU ship on which 4,000 TEUs are on there before it comes to the United States. All of a sudden that ship comes into a port and picks up 2,000 containers of DOD assets and one of those previously loaded 4,000 TEUs has some kind of weapons of mass destruction in it. It gets out into the sea, blows up, and sinks the ship -- sinks those 2,000 containers that were earmarked for our ability to project force in the future. We have to be able to put those technologies in place where we can see those things and can detect, monitor, sniff, image, and conduct security audits across-the-board. We have to be able to develop security technologies that are non-intrusive. Right now, it is very intrusive.

How many of you have gone through the airport screening process since 9/11? I just came in on the red-eye and I thought I was going to get strip-searched in LA. The thing is that we have to move away from the intrusive kind of security. Whenever something is intrusive, it is because we didn't react to it. We need to be proactive in security technology and that technology has to be non-intrusive and it has to be transparent to you and I out there in the trenches. If we are going to look and focus on this technology, we don't need intrusive technologies – we need non-intrusive, transparent technologies that go on and do it as we are doing our business.

Thank you.

Carl Trovato, Director of Operations,
Philadelphia Regional Port Authority & AAPA

I was asked, what my role is with regard to security after 09/11. Being in operations, I would have to say that I'm probably going to be trying to maintain a balance between the security ethic, which, if our security people had their way would involve measures that are so tight that very little, if any, cargo would flow efficiently and the operations ethic, which is to move the freight on and off the ship, in and out of the gates as soon as possible, no matter what. In that lies a balance of security versus operations.

We all know that port facilities move freight in international trade and anything you see or touch, if it is not manufactured, grown or otherwise produced in the United States, Mexico or Canada, comes through one of the ports. Again, the challenge is to balance this facilitation of trade against the need for the security, with whatever measures and technologies we are discussing here and do it as soon as possible.

Ports have taken measures to secure their facilities, but the various federal agencies must take the lead in protecting the international borders. The FBI is the lead agency with terrorism and INS on border integrity. The U.S. Customs Service takes the lead in inspection of cargo. The Coast Guard is responsible for protecting the domestic waters and the waterfront facilities. These agencies must be provided with the necessary resources to do their job. I think I'm preaching to the choir here, but I have to say that this includes funding existing programs that can improve the safety and security of our ports and the technologies that are needed to collect data on imports and exports, track vessel movements in and out of the port, and push that awareness as far away as possible from the physical borders of the United States.

The AAPA has been an advocate over the years for increasing funding for these various programs, including grants for establishing new technologies. However, we have to remain focused on some of the many federal programs that have not had sufficient support in the past. They are out there somewhere, and I would like to mention some of them.

Funding for the U.S. Customs Service's Automatic Commercial Environment (ACE) system – I don't know where that is going, but they need that for clearing imported cargo. Funding for additional surveillance equipment is necessary. In Philadelphia, the Customs Service has two electronic surveillance machines – they are not really x-ray, but they are a combination of x-ray and gamma. We have these for the whole port and that includes Wilmington, Camden and Philadelphia. I asked the Customs people how much more equipment would they need to do the job efficiently. I was told that along with the equipment, more personnel are needed. It is fine to throw money at it, but the equipment is only one part of it. It is also requires more people. Right now they are using Air National Guard out of Phoenix to help them test this equipment. There is one machine that can inspect a container in two minutes, and analyze and decide whether it is good or not in six minutes, which is a whole lot better than the intensive exams they used to do that take 1-2-3 hours. This equipment and technology is not cheap. One of the larger pieces of equipment goes for about $4.0 million and a smaller unit is $985,000.
There are also some other programs that are out there that have not come to any conclusion. One of them is the U.S. Coast Guard's automatic identification system (AIS) and vessel traffic management system (VTS). In order for the Coast Guard to realize they have the vessels out there and be able to decide whether or not to let the vessels in, it would be helpful if they could have this technology at their fingertips. The other one is the NOAA PORTS system which gives you real-time tide and current information, which also helps. That is another technology that is there, but it hasn't been fully developed.

What have we done since September 11th at the Port of Philadelphia? We have addressed the conditions of our waterfront facilities. In fact, the interagency report that came out said some of our facilities are less than adequate and if Customs had their druthers, you would have some bonded areas. We have addressed all of the perimeter fences, the gates, and tried to button up the envelope so that we could at least have an adequate physical barrier to unwanted access to the facilities. We have also been working with the individual terminal operators to institute sufficient ID badges and auto-pass systems. However, the other side of the fence is that now I have at least five pieces of identification. It would be nice for the technology people to come up with one type. I have one that is a bar code system; another one is electronic; another one is a magnetic type. It would be nice if we had one badge that you could go to any one of the facilities and wave it and get on.

PRPA also has, through state funding, undertaken an extensive study to analyze our present port security system. We've performed vulnerability and threat assessment and there will be recommendations made for changes to our current security to meet the demands of this heightened awareness. As Tony mentioned, the Coast Guard just can't handle assessments on all the ports right away, so we have undertaken that. The Port Authority is also working with the U.S. Coast Guard and other federal and state local agencies to create a port-wide security program – to gather information, disseminate anti-terrorism information throughout the seaport itself, with the institution of the local Port Security Committee.

The bottom line is that we have to continue to move the freight. We have to get the results to ensure we can keep the commerce of the United States moving and to do so will require using all these technologies. Thank you very much.

John R. LaCapra, President
Florida Ports Council

I have learned the two key words that perhaps best describe what we all have been feeling in Florida about our state of affairs. Yesterday, the Commandant of the U.S. Coast Guard told us about an altered state of thinking as we approach maritime movements and security. The Captain this morning told me we were in a “new normalcy”. What I think that means is an altered state of thinking. We are in a new normalcy and it describes what we have been feeling in the Florida port system.

Florida Ports Council is a facilitator. We are problem-solvers. We take the tasks that ports need to have done as local entities and we translate those tasks to both the state and federal system, and we produce money, and we solve problems and we move on. I think that is what everybody is trying to do here – move on.

What we have learned about the new normalcy in Florida is that today we are field commanders. What do I mean by that? I give you a real-life example. Recently, I walked into a room with the state head of law enforcement, the Admiral from the Coast Guard region, the National Guard Generals, eight different sheriffs, local law enforcement, the Governor’s office, and the Florida Ports Council, talking about deployment of the National Guard at four of our high-risk ports -- deployment called by the U.S. Coast Guard. Simply put, we don’t have the ability to take care of new deployment of shipping into these ports. That new deployment was also for the cruise lines who leave other places in the world and come to Florida during the winter. They were bringing a new forced deployment that required manpower and the ports had to answer the manpower call. How do we do that?

Somebody had to ask the Governor to pay for it. I had that opportunity and he basically said, we don’t have the funds. This is not a federal call-out. The state is going to have to pay – you’re going to have to find the money. Ladies and gentlemen, I don’t see in this audience the people who are going to wind up paying for this yet. They should be here. They should be part of this process because somewhere down the line, everybody who is talking here is saying somebody is going to pay for it.

I went to one of the industries that I think understands the law of business – you either pay me now or pay me later – I went to the petroleum industry and said look, you have a trust fund – you’re going to provide the money because we are going to deploy the troops. The troops are being deployed in Florida now to handle this augmentation of Coast Guard forcing, hopefully Customs forcing as well, because we know we are asking them to do certain other things with containers, and to handle the new realities of Florida’s position.

Florida did pass a law requiring security plans. These security plans have minimum standards. They require restricted access areas and we have badging and background ID checks that will be implemented by January 1, 2002. We do have technology to take of uniform badging. Again, the new altered thinking – but it really was there all the time for seaports. All of our customers, a wide array of customers (petroleum and cruise industries, containerized cargo movers, trucking is a member of the marine transport system and so is rail), have all come to us and said they don't want to have multiple badges. I will tell you that on January 1, Florida will have a uniform badging system in place or almost in place to handle the needs of continuing to move better, faster and cheaper.

I want to talk about better, faster and cheaper because in an altered state, and under new normalcy, perhaps we will have to pause on that subject of moving freight in that way. We are going to have to ask who is going to pay for security forces that seaports have never been trained to provide. One recommendation offered to Coast Guard and Customs is a training course for port directors who have never been trained in security the way we have security today. Nonetheless, they have been asked, and they will be asked, by federal law and state law to provide security, to provide minimum standards. Let me tell you what the new technology is. I am rest assured that USTRANSCOM and others will find us the new technology. But, let me tell you what the new technology is today – it is really old-fashioned technology – it is shared information, shared planning and shared communication. A lot of these people who are in charge of security never did that before September 11th.

We, in Florida, had to do that before September 11th because we had a law that was passed, and believe me it was not easy getting everybody to the table to talk. I want to compliment our state law enforcement people because they made the effort while they were working at each port, doing assessments, they made the effort to bring the other parties to the table. That is why as field commanders today – ports are the field commanders – we were able to walk into that room and agree upon deployment of personnel assets.

We need better deployment techniques and they have been talked about. We certainly need to help the agencies that provide our first-line of protection and information about risks. In this process, I am concerned about who delivers that message to the U.S. Congress. Customs and Coast Guard? I've been asked to testify in Florida on three or four committees in the last month about how are we going to fund our risks? How are we going to pay for the people? The first thing that I'm forced to say is that I think this is a federal obligation and we must first understand what resources they are going to put on the table. We can't fill a gaping hole unless we understand what commitment the federal government is going to make.

Yesterday afternoon, I spent a lot of time and before that the previous week walking the halls of Congress, trying to find them in cubby-holes, now that they have been dethroned from their rooms, and trying to get the message across: when are you going to pass this because this is really serious. It is serious when you walk into a room with all those people and we're talking about deployment of troops. It is serious. Someone has to deliver the message and I would hope that the U.S. port system, and certainly the Florida ports are going to deliver the message. We are there already and hopefully we are going to deliver the message that we need resources for Coast Guard, for Customs, for INS, and for anybody else who is going to provide the first line of protection. I am glad to see that all the consultants in the world who were preaching better, faster and cheaper are now in the security business, realizing that is where the new economy is. They better be out there preaching, because they won't do business in Florida unless they are preaching that type of message.

The private sector is really the force that needs to deliver the message. In this marine transportation -- I don't know much about the federal process, but I do know something – you better bring those parties to the table because they are going to pay for this a year from now. If you tell them they're going to pay for it, they will come and they will show you how to get it done. They will make government move at a faster clip to provide the things that you've talked about here today. I encourage you to bring them to the table. We bring them to the table in Florida and that is why we have been successful in doing the things we have done.

We do have funds; however, they are never sufficient for this. There is one other item of technology that I wish to command to you and that is eyes and ears. One of the issues that we came across in Florida that was very difficult for us, because we do have ID background checks and labor. Because Florida is very much into drug interdiction issues, the first element to touch cargo in some way was identified as being a problem to us. Law enforcement also had a role in this, but law enforcement wasn't in our seaports. They didn't come on the seaport. That was a difficult issue. Why didn't law enforcement come? Because there was no incentivization. As you look and plan out there, incentivization is an issue and in the federal process I would hope that labor would come to the table, so that they would be incentivized, and that they would be eyes and ears and help us in this process, as everyone should be.

We struggle now with the new way of thinking. Better, faster, and cheaper was a mantra that we at the Florida Ports Council preached. We were successful in forging a partnership with the State of Florida where over $1.0 billion was put into infrastructure. Now some of that infrastructure money is going to have to go to security infrastructure and technology. Does that mean we will be delaying better, faster and cheaper? You're darn right it does. As we look at this issue of security versus trade and keeping that balance – aren't we really re-thinking in an altered state about how we move commerce? Isn't it time for all of those people to come to the table because they are the ones who demand the just-in-time? Isn't it time that those shippers and those carriers and all those other modes come to the table and figure out how much they are going to pay for this? Aren't those the messages to deliver to Congress and other government agencies about what we can afford and how we can afford it? I think they are and I think that is the altered state we are in, and that is the new normalcy.

Thank you very much.

John J. Lynch, Special Assistant for Force Protection, NAVFAC, U.S. Navy

I will begin by telling you about NAVFAC and what we do. We basically provide the engineering solutions for the fleet, and in this particular case, for port security and waterside protection. We work with the fleet, CINCLANT, PAC fleet, major claimants. We work with base security. What they do is they provide information for us. They provide the asset. They provide us the level of protection that we are looking to protect from. Then, what we do is look to the engineering solutions. By doing that, we look for the engineering solutions on the technical side of providing criteria and guidance and policy. In doing that, we work with the base security, the intelligence community. We also work on the technology side, working with the different agencies – the Army's labs, the Navy's labs, and the Air Force labs, and coming up with technologies and funneling it all into an engineering solution for, in this particular case, port security.

For port security, what we are looking at is a whole program. For the waterfront plan, we are looking at a five-phased plan. That plan is to deter, to detect, deny, warn and then destroy if possible. The way we are doing that is through harbor patrols. We are looking at barriers and boundary lines and demarcation lines. We are looking at it through a wide communications system between the shore and the ship and port operations and security operations and roving patrols, and the maritime community and the Coast Guard. We're trying to put everything together into one simple program that will cover everything.

Right now for the waterside, we are ahead of the curve. We were doing a lot of this stuff way before 09/11. Right now on our piers, we do have existing security measures. We have minimal lighting. We have some communications. We have pier access control and guard shacks. Most of our piers now are being designed that we are going to have guard shacks and permanent vehicle barriers – either gates, pop-up barriers, or crash gates. We have a telephone system and we have a fire alarm system, all required by Code and required by our criteria.

What we propose in the future is to provide capabilities for our waterfront boundaries and waterfront barriers. They may be marine platforms, waterfront platforms, or mechanical systems, winches and boats to provide support for our barriers. We are looking at putting waterside towers at selected piers for overseeing vessels, possible terrorist activity. We are looking at increasing our lighting. Right now, we basically have lighting out there for safety, as required by OSHA. But, we are looking at multi-level lighting systems that will provide, at the touch of a button, we can increase the lighting levels to provide security, and to look out to the water and see what is out there. We are looking at expanding communications and cabling systems. We are looking at systems to provide communication between all the assets down at the waterfront and also we are looking at increased harbor patrols.

Waterfront security – what do we have right now and what are we working on? Right now most of the AOR for the CINCLANT fleet and some for the PAC fleet have some type of float line as a boundary or demarcation line, identifying an area that is restricted for Navy property. We are working on port security barriers. We are working on other barriers and boundary lines, such as tug-float system in ________

We are looking at signage at the Navy. All piers on the waterfront have well-lit signage indicating "keep out" areas. We are looking at watchtowers and at guardhouses at the end of our piers and at the foot of our piers. We are looking at vehicle barriers, both at the pier gates and our main gates. At selected gates during certain threat times, we are looking at putting vehicle barriers in place. We are also looking for increased lighting and increased communications as well.

Right now at the Naval Station Norfolk, we have a boundary line that consists of a float line and buoys that are painted yellow for identification and markings. We have stainless steel cable supporting this. We have a polyprophalene line that helps floatation and identification. These lines are in the water right now. They are supported and connected by mooring buoys about every 500 feet. These lines are lit and, in some cases, are well signed.

We're working on barriers and the effectiveness of our barriers. Right now, we go from a 1 to 5 effectiveness. The boundary lines that we have right now are a 5, which is the lowest. We are working on boundaries and barriers in the 2-3 range or 2-4 range, and we are right now testing barriers in the 1-2 range for effectiveness. The barriers from 2-4 we're working on putting those barriers out and working them with the comprehensive systems: the communications, the harbor patrols, the roving patrols, the pier guards at the end of the pier.

The effectiveness of #1, which is going to stop a boat, has been tested. We have been testing these for the last decade and we are coming up with better systems using better materials.

We are already in the testing mode on a rank #1 port security barrier. We have tested this for small craft at a high rate of speed, and it has worked. It has stopped the boat. It has stopped the threat. Currently, we are getting ready to install this barrier at a southeast installation, testing this barrier for operations, and testing it for maintenance to see how it works. Another barrier we are considering is the dumma barrier, which is a floating bladder. This barrier system is used in the U.K. at the submarine base and it is highly effective. We have tested this and it does stop a boat. It has ratings of a 2. For a higher threat, it is questionable and we are doing more testing. Both of these systems, the dumma system and the port security barrier, have been tested at 110 and 156 scale models for operations for testing, for movement, for gate systems and it has proved helpful in the design of these systems.

We are also looking at other boundaries and barrier systems. On example is a tough float system that we are testing currently in the northeast area, which has a very high current rate. It is being battered and it is being tested and it is marginal in that we are working on other systems such as a a fender system, a camel-type. In the Norfolk are, we are also testing a Yodock system, which basically is a vehicle barrier that has been modified to work as a water barrier.

One of the criteria issues that we need to look at is threat. Exactly what are we trying to design our barriers for? We are looking at the barrier effectiveness. What kind of craft are we going to look at? How is the effectiveness? Is it going to stop it? How much penetration is required? We are looking at the environmental design criteria. What is going to be needed to support these barriers? What kind of systems – is it going to effective the environment? Mooring design criteria – what are we looking at? Are we looking at a mooring platform to support these, or are we looking at dolphins or are we looking at simple mooring buoys and anchor systems? We are looking at public safety requirements, working with the Coast Guard. Is it well lit? Is it well signed? Is the public aware that these boundaries and these boundary lines are out there? We are looking at permitting. If we start doing work out in the water, what permitting do we have? Do we need EIS and EIAs – environmental impact statements or assessments?

All this gets down into the costs. We are looking at the initial cost and then we are looking at the life-cycle cost. What is it going to take to support these boundaries and boundary lines? Life cycle cost includes operations and maintenance and that is what our testing is all about. We are looking at the operations and maintenance. These are systems that have never been deployed in the Navy or the private sector, so we are really looking at our testing sites now to see these operations and get feedback from the port operations people and the port operators.

We are going back to basically the tradition of measures for security. We are looking at watchtowers at selected parts of our pier. Again, this is for surveillance of ships and personnel and unauthorized vessels in the water. We are looking at permanent-type construction at the end of these piers. We are looking at bullet-resistant type construction. We are looking at providing all the manpower and equipment required for a 24/7 type of operation for these facilities. We are looking at pier guard shacks at the end and at the foot of our piers. One example is a semi-permanent guard shack that provides shelter and some resistance. It has radio communications with the ship and with the harbor patrol. We have an enunciation system quite loud at 118 decibels. It provides a number of warnings if craft approach a Navy-restricted area.

We are looking at gate barriers at the foot of our piers. We are looking at personal access control using access control cards. Some of the gates weren't designed for a specific threat that we are looking at, and we are looking at right now to reinforce these gates. We have permanent guard shacks. As I mentioned earlier, all our new piers are being designed with vehicle barriers and guard facilities. The vehicle barriers are crash-type gates and pop-up type vehicle barriers. These are at selected gates at the foot of our piers and some of our main gates of entry into the waterfront facilities.

We are looking at increased waterside security lighting. Again, the purpose is to provide multi-level security lighting, identify and locate vessels within the restricted area, and surveillance. Again, light intensity can be coordinated. We are looking at coordinating this lighting intensity with our port ops people and the pilots. We don't want to blind them.

We are looking at expanded communications systems to provide communications between our port operations, between the security operations, and between ship and the shore patrol, and between the piers.

We are looking at signage. Again, once we identify what our support system is for our water barriers, we will have signs. This is to be a three-sided sign, well lit and enforceable.

Finally, we are looking at increased harbor patrols. This is the last, but not the least. As mentioned earlier, our harbor patrol is 24/7 and to do this, we need additional craft and additional personnel. Right now, the Navy and the other services are running thin on people and facilities.

Thank you.

Raymond Barberesi, Director, Office of Ports and Domestic Shipping, Maritime Administration

It has impressed me since the beginning of the marine transportation system initiative how strongly people feel about being at events. Right now, our country is at war and we have, in Tony Regalbuto and John McGowan, two people who have this finger on the pulse of what is happening in security in this country today. Tony is the Director of Security for the U.S. Coast Guard. John is the Executive Director of Enforcement for the U.S. Customs Service. They think it is important enough to be here this morning.

What is important at this conference and what we're doing here is to learn from one another. There are a lot of technologies being developed and marketed out there. In the last two months, I've heard of more things from more people than I ever knew existed. They can tell what color your fingernails are if you hand is in your pocket when you're going through the airport. It is out there and what we really need to do is collaborate and get it together.

I want to talk to you a little bit about what MARAD does in the area of port security and how that plays into the MTS and the R&T roles that we are discussing in this forum. We deal with commercial readiness and military readiness, research and technology and legislation.

With regard to our respective roles, under MTS we have the National Advisory Council, the non-federal stakeholder group that is sponsored by MARAD and the Interagency Committee for the MTS, which is headed and chaired by Admiral Pluta of the U.S. Coast Guard. I might mention that RADM Pluta was ahead of the Office of Homeland Security in getting together the public stakeholders in the security committee forum to develop a matrix of what is everyone doing out there. There is a lot going on and we know there are things going on, but in the federal government, if you can believe this, sometimes we don't know what the other folks are doing. Through the Coast Guard and Admiral Pluta's leadership and the Interagency Committee, we are developing a matrix to find out how we all can work together. I heard some things from John Lynch that the Navy is doing that I haven't seen before, and we need to better coordinate that.

Port security guidance to U.S. ports – we need the mechanisms to share best practices. I recently spoke to a port director who said after the terrorist attacks of September 11th, they have obviously been spending a lot of money to raise the security issue and to raise the effect of it. He indicated that after six weeks, they did a little study about how that all looked, and they figured they were spending 70% of what they spent for nothing. This is not to say it wasn't necessary. The point is there are a lot of things going on within our ports and it is important to know from the ports themselves what works, what is or is not effective and the best practices that are out there and learn from each other. This needs to be better coordinated.

A couple of years ago, MARAD prepared a national planning guide. It is done under the auspices of the U.S. Department of Transportation whether or not we get funding for it. We need to do something like that again to put a focus on security. Also, the U.S. Merchant Marine

Academy at Kings Point does industry security training and they are ready to continue that process and expand it.

I mentioned homeland security roles. We glean this from Governor Ridge's Office of Homeland Security and what his efforts are and what he sees as security needs for the United States. We need to be prepared. We need a strategy and we have to be prepared and we have to have mechanisms to prevent bad things from happening and that Office of Homeland Security is a place where all that can be coordinated.

Regarding international roles, foreign port security is very important. In my former life when I dealt with national security at MARAD, I used to go out to TRANSCOM those folks really instilled in me that when you go to war, you want to play an "away game". It is true when you go to war and it is true when you're thinking about security – we want to be able to reach out and touch someone when they are over there, before they get here, and do something bad here. That is an essential element and a lot of folks have touched on it today and we really need to look at that.

At MARAD, we have worked with the Peruvians under the U.S. Southern Command and in coordination with a lot of other federal agencies, to do port assessments down there last year. The Caribbean Third Border Initiative is another multi-agency tasking, under the State Department, where we try to get bilateral benefits from our partners in this hemisphere. One example is the Jamaican Marine Transportation System Initiative. Prior to September 11, the U.S. Secretary of Transportation signed a Memorandum of Cooperation with the Minister of Transport of Jamaica. Our delegation is led by the U.S. Coast Guard. There are people out there in the world that want this transportation system to work, and they want it to be secure and they wanted it that way before and they want it even more now. We are getting approached by more governments of other nations after those events in part because they feel if this can happen to the United States of America, it can happen anywhere.

MARAD also heads the U.S. delegation to the Organization of American States' InterAmerican Committee on Ports and chairs the Technical Advisory Group on port security. Under the OAS, MARAD also manages the port security training program. We talked about training and how important it is. In the last couple of years, we have managed over nearly 300 folks being trained in port security issues in this hemisphere. This is something that is going on and maybe people don't know about it – something that can be expanded. I keep thinking about AAPA and I'll admit this before I got specifically into the port business, the American there is the Americas – it is everybody, not just the United States. It reaches out to our foreign partners too. There is an organization that can assist in making sure that the world and the transportation system is as safe and secure as we can get it.

On the military front, security for port readiness is absolutely essential. I have a fear, as do a lot of folks, that what is happening right now in Afghanistan is at a low level and we would really like to have it stay that way. But, if it escalates, it will escalate quickly and we need to have a transportation system that can deploy our forces and equipment as quickly as we need to. The National Port Readiness Network is chaired by the Maritime Administration. We partner with nine federal agencies, a lot of them which are sitting up here with us, to plan with 13 strategic ports and whether that number is right or enough is also a think we should be talking about and need to take issue with. What I really think we need is to have all of our ports ready and prepared to really take care of any contingencies that might happen to us. We train federal port controllers. We provide secure communications for them.

The last thing I want to mention is the port initiative – something that through TRANSCOM and the Federal Highway Administration and the Coast Guard and MARAD, we are looking at the whole string of a transportation system. It is the whole transportation system that needs to be secure.

In time of war, a large part of MARAD turns into a completely different entity. Not a lot of people know that. I don't like to think about it because I kind of like my job and I'm hoping we never get to the point where we have to turn into the National Shipping Authority. But, that is the role that MARAD plays. MARAD has authority not only to provide a civilian sealift to the Department of Transportation during contingencies, but we also have authority for providing port facilities in support of actual emergencies. We like to do those things in a partnership where we can do them to everyone's benefit. We would not like to do it, but we are prepared to do it. Keith mentioned earlier the Ready Reserve Force. MARAD maintains and manages that force to be delivered to DOD in national emergencies. Keith also mentioned the Center for Commercial Deployment of Transportation Technology (CCDOT) program – agile port technologies, rapid deployment technologies – a DOD funded program. TRANSCOM and MARAD partner in this with California State University at Long Beach. It is a great program for transportation technologies to move our troops out and our equipment out faster. At MARAD, we also have cargo handling and ship operators cooperative committees that are working on some things related to our security efforts.

Last but not least are the items in port security legislation. One that is kind of controversial is port employee accreditation. It is not only about port employees. It is about transportation system employees. So many people touch freight that many feel there needs to be a national look at accrediting people who touch that freight and deal with it.

I would like to point out that there are some things going on in the MTS network, especially in the R&T subcommittee to get studies and technology that is out there to a place where everybody can at least see it and to try to develop it. Someone recently asked me what I felt was the most important thing in terms of port and marine transportation system security and I said information. We need more and better information. We need a better way of sharing that information. We need a better way of having that information available to the appropriate people, and we need to be able to train analysts to assimilate that information and the hardware to detect bad things. We need to do that, though, in a way that doesn't work to the detriment of the commercial marine transportation system. It is a tough thing to do, but we need to do it. Our security has to go to both our national security and our economic security. We can do it and the people that are out here can do it.

On September 11th, thousands of our countrymen died in the most horrific largest single-assault on this country that we ever experienced. We here can do something about securing our transportation system and making sure their lives were not lost in vain.

Thanks very much.

Summary of Q&A Session

Q: I had a question with regard to a comment made in the introductory remarks, about pushing our borders and our sensors further out to sea and the ability to detect such things as weapons of mass destruction at the sea buoy. Yesterday, someone talked about the intelligent waterway system, and as part of that we have been conceiving things like a buoy information network where you instrument buoys with smart sensors. In the past the idea has been for navigation safety and application. Do you see the fact that we have an estimated 50,000 floating aids out there as potential platforms for sensors like you're discussing? Could the buoys themselves be platformed with these sensors, given the shortage of other resources?

Response: There is no question in my mind that they can be and that is what we had in mind. Also think about all of the offshore platforms that we have in the Gulf. We have been talking with that industry and we're looking at putting sensors out there, including radar and getting better visibility out there. We certainly want to prevent a Kuwait-type accident with the offshore platforms. There is some talk of moving LNG offshore too. Certainly, we are going to have to look at protection that far out on our coastlines. We will certainly need that domain awareness.

Q: Does the U.S. have the authority and systems in place to look at the bios of the officers and crew of some of the commercial vessels that are in U.S. waters, in view of possible sabotage?

Response: That is a major problem internationally that was alluded to earlier. We can do the screening on those people that are coming in, assuming that is the person that is presenting himself/herself. As far as I know, there is no process in place to do criminal background checks to that degree that we do on our U.S. seamen. It is certainly a loophole that has to be addressed internationally.

Q: It was stated that with regard to inspections, you want to push off the inspection off our borders as far as possible. Several people brought that up. In light of that statement, do you plan to do anything about that at the point where/when the container is loaded? As an example, could you address a container load of automobile parts from Mexico or coffee from Colombia?

McGowan: What we already have in the counter-drug environment is what we call the industry partnership programs. We have carrier initiative programs, and we have something called the business anti-smuggling coalition. These are voluntary programs. We educate the manufactures and the people who are in the transport chain. We give them checklists so that they can protect themselves. We give them scenarios that they can run through. The ones who adopt it are successful in keeping better control of their commodities from the time it is manufactured from the time it is imported. Unfortunately, they also become targets if they look like they are in a faster lane than the rest of the cargo, if they look like they are not being examined. I can tell you this based on our experience in the south cross-border. They do become targets of people who want to top-load legitimate cargo with contraband. We find a significant amount of cargo that has been manipulated, seals that have been manipulated, drivers who have been paid off. You have to balance that capability with some sort of checks behind and that becomes more difficult as we expand the areas of risk. We were talking about a pretty well-defined practice – as I mentioned, there are only a few places in the world where cocoa is grown that make the cocaine. There are a lot more places where we're going to be seeing terrorist activities because they will find sympathetic cells within a wide variety of countries.

I talked about trying to segment our risk. One percent of the containerized cargo that comes into the United States arrives by vessel from the Mideast. Three percent arrives by vessel from about 54 countries that have active Al Qaeda cells that can probably generate some mischief. I don't know where else they might be. I don't believe we are going to see a front-on attack. I think we are going to see triangular trade. We are going to see trying to commingle with the broad majority of legitimate cargo. We are going to be meeting and dealing with major importers who deal with a lot of different manufacturers in a lot of different countries, and we are going to be talking to them about things they can do. That is not going to push off inspection foreign. It is just going to start tightening up the transport chain. You have to make a decision somewhere in the business that you're going to protect your brand name and the protection of your brand name might incur more costs in your transport chain. I think those decisions have to be made.

There is a lot of pressure on the Customs service to not cause just-in-time inventory procedures to be totally bollixed up. I talked up earlier about the just-in-time inventory system on the automotive manufacturer – it went from three hours to eight days. They didn't like that. We recognize that we have a commitment and a responsibility to a safe, secure, porous border, and that is a very difficult task. We need a lot of coordination and cooperation from all the players.

Comment: I would also like to comment on that. In some of the draft legislation I've seen, there could be a requirement to do foreign port assessments, and I would envision that would be obviously Coast Guard, Customs and INS, to do an assessment of the foreign port to see if they have adequate security and provisions in place. For those countries that do, that would certainly fast track cargoes coming in from those countries, particularly if they were inspected at the point of loading, had electronic seals and had a good chain of custody of the container coming through the transportation system. Also in draft legislation would be the authority to accept or deny entry of cargo from certain countries if there is not adequate security. This would be a pretty strong hammer for those countries that do not play by the rules. If the legislation passes and we choose to exercise that authority, it is certainly a very important tool in our tool bag.

Comment: Many of you may not have traveled to Nigeria, but for the last five years or so or even longer than that, you have probably been in international airports where flights departing international, you have seen advisories posted by the Department of Transportation that says that Nigeria's major international airport does not meet U.S. standards for security. That is a strong statement and makes people think twice about traveling to Nigeria by air.

I also want to mention a point made earlier about the potential for a WMD in a container. What could you give a vessel operator or what capability should that vessel operator have while at sea to continuously scan his cargo? I want to call attention to the battery-operated personal radiation detective devices that can be work on a belt. You give one to the mate and he spends his whole time while at sea climbing around the vessel looking at the latching, making sure he is not losing any of his cargo. While at sea, there is a lot less radiation available generally in the background noise. Those PRDs are more efficient in that environment. Should we be giving or asking or contracting the carriers to operate in that fashion in the future? What other detector capabilities are needed, such as chemical and biological? Where is the chemical detector capability? As far as I know, we have no chemical detection capability while it is sealed. We have it after emission or after it has been released, and that is in a general environment capability, but we have nothing that looks inside the containers.

Comment: For the last two and one-half years I've been working in Central America with five Central America ports in Honduras and Nicaragua. The Port of Cortez is a hub port and, to make a long story short, we were there because of Hurricane Mitch as part of an interagency team, including industry. One of the results of that was a sister port agreement between the Port of Miami and the Port of Cortez. They have an ongoing technical training, interoperability in terms of equipment, and port security was one of the top issues that we identified. On the team I had a Coast Guard team that actually did the port security assessment. With the concept of keeping the threat beyond our borders, it seems to me that the concept of hubs around the world where there is a lot of interchange between U.S. port and foreign ports, that the sister port agreement, which is obviously something within the industry framework, might be another tool that we could add.